Deutscher Bundestag **Drucksache 19/12182**
19. Wahlperiode 06.08.2019

Kleine Anfrage

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller, Marcus Bühl, Jörn König, Wolfgang Wiehle und der Fraktion der AfD

Überwachung von Mitarbeitern durch Diensthandys und andere PC-Tools im Spannungsverhältnis zum Datenschutz

Nach der Wahrnehmung der Fragesteller sind Installationen von Überwachungstechnologie im öffentlichen Raum ein gewohntes Bild und begleiten nicht nur Ausnahme- sondern lebensalltägliche Situationen eines Bürgers: Kameras finden sich auf Flughäfen, in Bankfilialen, auf Bahnhöfen, vor Geldautomaten, in U-Bahn-Stationen, in öffentlichen Gebäuden und vielen anderen Bereichen des öffentlichen Lebens. Doch die Überwachungstechnik macht auch nicht vor den eigenen vier Wänden halt. Spätestens seit der Markteinführung von so genannten Smart Speakern und sprachgesteuerten, internetbasierten intelligenten persönlichen Assistenten wie „Alexa" hören immer öfter Unberechtigte mit (www.smartdroid.de/assistant-google-mitarbeiter-hoeren-mit-was-nicht-weiter-ueberrascht/).

Die technischen und digitalen Überwachungsmöglichkeiten beschränken sich allerdings nicht nur auf öffentliche Plätze und die Wohnung, sondern greifen schon längst auch auf den Arbeitsplatz über. Deutsche Unternehmen scheinen leider hier keine Ausnahme darzustellen.

Ein dienstlich genutztes Smartphone oder die Navigationssoftware im Dienstauto können dem Arbeitgeber eine Fülle von Daten übermitteln. Das kann dazu führen, dass der Arbeitgeber mehr Informationen zur Verfügung hat, als jemals zuvor. Zum einen kann die Überwachung von Arbeitsplätzen durchaus zweckmäßig im Sinne von Arbeitsabläufen und zur Verhinderung von Straftaten beitragen, allerdings wird in letzter Zeit vermehrt auf die Überwachung von Mitarbeitern gesetzt (www.manager-magazin.de/premium/ueberwachung-audiostory-sie-kennen-dich-sie-kriegen-dich-a-93348364-075b-4793-bc9a-452d89b21d74).

Mitarbeiter, die softwaregestützte Technologien nutzen, um beispielsweise Ein- und Ausgänge oder Login-Verhalten zu kontrollieren, haben die Möglichkeit, detaillierte Mitarbeiterprofile zu erstellen.

Die Überwachungsskandale wie die der Deutschen Telekom AG (www.manager-magazin.de/unternehmen/artikel/a-555158.html), der Deutschen Bahn AG (www.zeit.de/online/2009/04/bahn-bespitzelung) oder des Lebensmittelkonzerns Lidl (www.stern.de/wirtschaft/news/ueberwachungsskandal-lidl-muss-millionen-strafe-zahlen-3762026.html) haben offenbar ihre abschreckende Wirkung verloren. In Unternehmen in den USA und Großbritannien werden E-Mails, Web-Browser, Chatprogramme, Anrufbeantworter aber auch soziale Netzwerke überwacht (www.manager-magazin.de/premium/ueberwachung-audiostory-sie-kennen-dich-sie-kriegen-dich-a-93348364-075b-4793-bc9a-452d89b21d74).

In Deutschland ist so eine Praxis der Arbeitgeber illegal, denn grundsätzlich dürfen keine Daten genutzt werden, bei deren Beschaffung das Grundrecht auf informationelle Selbstbestimmung gebrochen wird. Zudem kommen gemäß der Datenschutz-Grundverordnung (DSGVO) dem Arbeitgeber umfangreiche Aufklärungs- und Unterrichtungspflichten zu.

Wir fragen die Bundesregierung:

1. Sind die in der Vorbemerkung der Fragesteller formulierten Umstände der potentiellen und teils umgesetzten Überwachungsmöglichkeiten der Arbeitnehmer der Bundesregierung bekannt?
2. Sieht die Bundesregierung bei der Transformation der DSGVO in nationales Recht gesetzgeberischen Handlungsbedarf, dass die persönlichen Rechte der Arbeitnehmer besser zu schützen sind?
3. Ist der Bundesregierung bekannt, wie viele Fälle vor dem Bundesarbeitsgericht in Bezug auf „Lauschangriffe“ auf Mitarbeiter verhandelt wurden?
4. Welche Maßnahmen hat die Bundesregierung umgesetzt, um Mitarbeiter des öffentlichen Dienstes vor solchen Übergriffen zu schützen?
5. Wie beurteilen das Bundesamt für Sicherheit in der Informationstechnik und der Bundesdatenschutzbeauftragte den derzeitigen Stand des Mitarbeiterschutzes in den bundeseigenen Einrichtungen?
6. Wie beurteilt der Bundesdatenschutzbeauftragte die Software Windows 10 in Bezug auf Sicherheit und Abhörsicherheit und deren Implementierung in der öffentlichen-rechtlichen Dienstbenutzung?

Berlin, den 16. Juli 2019

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333